Chapter I
RISK MANAGEMENT FUNDAMENTALS

1. Background

Risk management is a process that assists decision makers in reducing or offsetting risk (by systematically identifying, assessing, and controlling risk arising from operational factors) and making decisions that weigh risks against mission benefits. Risk is an expression of a possible loss or negative mission impact stated in terms of probability and severity. The risk management process provides leaders and individuals a method to assist in identifying the optimum course of action (COA). Risk management must be fully integrated into planning, preparation, and execution. Commanders are responsible for the application of risk management in all military operations. Risk management facilitates the mitigation of the risks of threats to the force. For the purposes of this document, threat is defined as a source of danger—any opposing force, condition, source, or circumstance with the potential to negatively impact mission accomplishment and/or degrade mission capability.

a. Each of the services uses similar but slightly different processes. This publication provides a single process to enable warfighters from different services to manage risk from a common perspective.

b. Risk management is useful in developing, deploying, and employing the joint force. Development concerns force design, manpower allocation, training development, and combat material developments. Deploying and employing the joint force generates concerns in force protection and balancing risk against resource constraints.

c. Military operations are inherently complex, dynamic, dangerous and, by nature, involve the acceptance of risk. Because risk is often related to gain, leaders weigh risk against the benefits to be gained from an operation. The commander’s judgment balances the requirement for mission success with the inherent risks of military operations. Leaders have always practiced risk management in military decision making; however, the approach to risk management and degree of success vary widely depending on the leader's level of training and experience.

d. Since the Korean conflict, United States forces have suffered more losses from non-combat causes than from enemy action. Key factors contributing to those losses include—

(1) Rapidly changing operational environment.

(2) Fast-paced, high operations tempo and high personnel tempo.

(3) Equipment failure, support failure, and effects of the physical environment.

(4) Human factors.

2. Risk Management Goal

The fundamental goal of risk management is to enhance operational capabilities and mission accomplishment, with minimal acceptable loss.

3. Key Aspects of Risk Management

a. Risk management assists the commander or leader by—

(1) Enhancing operational mission accomplishment.

(2) Supporting well-informed decision making to implement a COA.

(3) Providing assessment tools to support operations.

(4) Enhancing decision-making skills based on a reasoned and repeatable process.

(5) Providing improved confidence in unit capabilities. Adequate risk analysis provides a clearer picture of unit readiness.

(6) Preserving and protecting personnel, combat weapon systems, and related support equipment while avoiding unnecessary risk.

(7) Providing an adaptive process for continuous feedback through the planning, preparation, and execution phases of military operations.

(8) Identifying feasible and effective control measures where specific standards do not exist.

b. Risk Management does not—

(1) Replace sound tactical decision making.

(2) Inhibit the commander's and leader's flexibility, initiative, or accountability.

(3) Remove risk altogether, or support a zero defect mindset.

(4) Sanction or justify violating the law.

(5) Remove the necessity for rehearsals, tactics, techniques, and procedures.

4. Principles of Risk Management

The basic principles that provide a framework for implementing the risk management process include—

a. **Accept No Unnecessary Risk.** An unnecessary risk is any risk that, if taken, will not contribute meaningfully to mission accomplishment or will needlessly endanger lives or resources. No one intentionally accepts unnecessary risks. The most logical choices for accomplishing a mission are those that meet all mission requirements while exposing personnel and resources to the lowest acceptable risk. All military operations and off-duty activities involve some risk. The risk management process identifies threats that might otherwise go unidentified and provides tools to reduce or offset risk. The corollary to this axiom is "accept necessary risk" required to successfully complete the mission or task.

b. **Make Risk Decisions at the Appropriate Level.** Anyone can make a risk decision; however, the appropriate level for risk decisions is the one that can make decisions to eliminate or minimize the threat, implement controls to reduce the risk, or accept the risk. Commanders at all levels must ensure that subordinates know how much risk they can accept and when to elevate the decision to a higher level. Ensuring that risk decisions are made at the appropriate level will establish clear accountability. The risk management process must include those accountable for the mission. After the commander, leader, or individual responsible for executing the mission or task determines that controls available to them will not reduce risk to an acceptable level, they must elevate decisions to the next level in the chain of command.

c. **Accept Risk When Benefits Outweigh the Cost.** The process of weighing risks against opportunities and benefits helps to maximize mission success. Balancing costs and benefits is a subjective process and must remain a leader's decision.

d. **Anticipate and Manage Risk by Planning.** Integrate risk management into planning at all levels. Commanders must dedicate time and resources to apply risk management effectively in the planning process, where risks can be more readily assessed and managed. Integrating risk management into planning as early as possible provides leaders the greatest opportunity to make well-informed decisions and implement effective risk controls. During execution phases of operations, the risk management process must be applied to address previously unidentified risks while continuing to evaluate the effectiveness of existing risk control measures and modify them as required.

5. Levels of Risk Management

The risk management process has two levels of application: crisis action and deliberate. Time is the basic factor that contributes to the selection of the level of application used.

a. **Crisis Action.** Crisis action risk management is an "on-the-run" mental or verbal review of the situation using the basic risk management process. The crisis action process of risk management is employed to consider risk while making decisions in a time-compressed situation. This level of risk management is used during the execution phase of training or operations as well as in planning and execution during crisis responses. It is particularly helpful for choosing the appropriate COA when an unplanned event occurs.

b. **Deliberate.** Deliberate risk management is the application of the complete process when time is not critical. It primarily uses experience and brainstorming to identify threats and develop controls and is, therefore, most effective when done in a group. Examples of deliberate applications include planning upcoming operations, reviewing standing operating procedures (SOP), maintenance, training, and developing damage control or disaster response plans.

6. Risk Management Process Overview

The risk management process involves the following:

- Identifying threats.
- Assessing threats to determine risks.
- Developing controls and making risk decisions.
- Implementing controls.
- Supervising and reviewing.

a. **Threat Identification and Threat Assessment.** These elements comprise the risk assessment portion of risk management. In threat identification, individuals identify the threats that may be encountered in executing a mission. In threat assessment, they determine the direct impact of each threat on the operation. Risk assessment provides enhanced awareness and understanding of the situation. This awareness builds confidence and allows timely, efficient, and effective protective measures.

b. **Develop Controls, Make Decisions, Implement Controls, Supervise, and Review.** These remaining elements of the risk management process are the essential follow-through actions of managing risk effectively. Leaders weigh risk against benefits and take appropriate actions to eliminate unnecessary risk. During planning, preparation, and execution, the commander should communicate his acceptable risks to subordinates and continuously assess risks to the overall mission. Finally, leaders and individuals evaluate the effectiveness of controls and capture lessons learned.

7. Risk Management Process Application Guidelines

This section provides general guidelines for applying the risk management process. To get maximum benefit from this tool—

a. **Apply the Process in Sequence.** Each element is a building block for the next one. For example, if threat identification is interrupted to focus control on a particular threat, other more important threats may be overlooked and the risk management process may be distorted. Until threat identification is complete, it is not possible to prioritize risk control efforts properly.

b. **Maintain Balance in the Process.** All parts of the process are important. If only an hour is available to apply the risk management process, the time must be allocated to ensure the total process can be completed. Spending fifty minutes of the hour on threat identification may not leave enough time to apply the other parts of the process effectively. The result would be suboptimal risk management. Of course, it is simplistic to rigidly insist that each of the parts is allocated ten minutes. The objective is to assess the time and resources available for risk management activities and allocate them to the actions in a manner most likely to produce the best overall result.

c. **Apply the Process as a Cycle**. See Figure I-1 below. Notice that "supervise and review" feeds back into the beginning of the process. When "supervise and review" identifies additional threats or determines that controls are ineffective, the entire risk management process should be repeated.

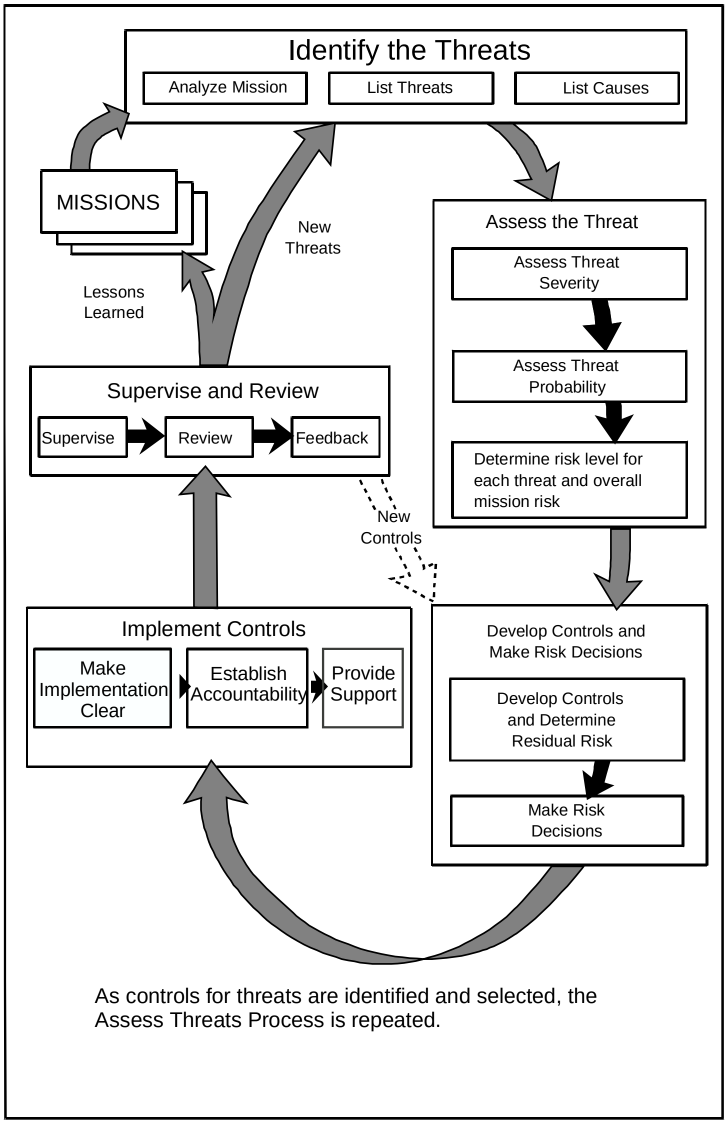

Identify the Threats
Analyze Mission
List Threats
List Causes
MISSIONS
New Threats
Lessons Learned
Assess the Threat
Assess Threat Severity
Assess Threat Probability
Determine risk level for each threat and overall mission risk
Supervise and Review
Supervise
Review
Feedback
New Controls
Implement Controls
Make Implementation Clear
Establish Accountability
Provide Support
Develop Controls and Make Risk Decisions
Develop Controls and Determine Residual Risk
Make Risk Decisions
As controls for threats are identified and selected, the Assess Threats Process is repeated.

Figure I-1. Continuous Application of Risk Management

d. **Involve People Fully.** The only way to ensure the risk management process is effective is to involve the people actually exposed to the risks. Periodically revalidate risk management procedures to ensure those procedures support the mission.

8. Relationship of Force Protection to Risk Management

The commander has the dilemma of weighing mission requirements and force protection measures. One of his primary tools for weighing mission and protection is reconciled by assessing and balancing risk. This process forms a direct relationship between force protection and risk management. In the force protection process, we consider three elements: planning, operations, and sustainment. Risk management enables the force protection process by using risk assessment and controls in each element. The relationship between force protection and risk management is evident in the following:

a. In planning, we conduct risk assessment and develop controls.

b. In operations, we update risk assessment and implement controls.

c. In sustainment, we continue to update assessments and adjust controls.

Chapter II
RISK MANAGEMENT PROCESS AND OPERATIONAL CONSIDERATIONS

1. Background

This chapter discusses the risk management process and how it may be applied in the planning and execution phases of all operations. This chapter also provides two situational analysis models. These models are the mission, enemy, terrain and weather, troops and support available, time (METT-T) model and the man, machine, media, management, mission (5-M) model.

2. Application of Risk Management

a. **Identify Threats.** A threat is a source of danger: any opposing force, condition, source, or circumstance with the potential to impact mission accomplishment negatively and/or degrade mission capability. Experience, common sense, and risk management tools help identify real or potential threats. Threat identification is the foundation of the entire risk management process; if a threat is not identified it cannot be controlled. The effort expended in identifying threats will have a multiplier effect on the impact of the total risk management process. Figure II-1 depicts the actions necessary to identify threats associated with these three categories: (1) mission degradation, (2) personal injury or death, and (3) property damage.

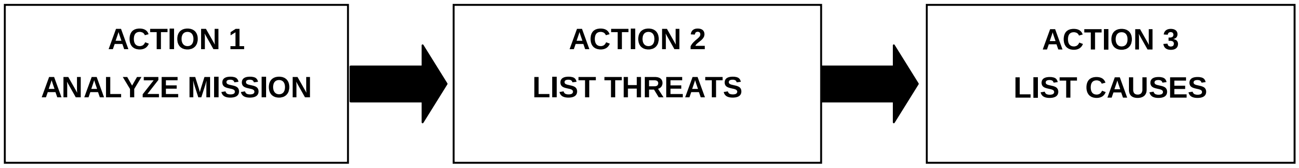


Figure II-1. Identify the Threats

(1) **Action 1—Analyze Mission.** This is accomplished by—

(a) Reviewing operation plans and orders describing the mission.

(b) Defining requirements and conditions to accomplish the tasks.

(c) Constructing a list or chart depicting the major phases of the operation normally in time sequence.

(d) Breaking the operation down into “bite-size” chunks.

(2) **Action 2—List Threats.** Threats (and factors that could generate threats) are identified based on the mission and associated vulnerabilities. The output of the identification phase is a list of inherent threats or adverse conditions, which is developed by listing the threats associated with each phase of the operation. Stay focused on the specific steps in the operation; limit your list to “big picture” threats. Examine friendly centers of gravity for any critical vulnerabilities. Threats may be tracked on paper or in a computer spreadsheet/database system to organize ideas and serve as a record of the analysis for future use.

(3) **Action 3—List Causes.** Make a list of the causes associated with each threat identified in Action 2. Although a threat may have multiple causes, it is paramount to identify the root cause(s). Risk controls may be more effective when applied to root causes.

b. **Assess Threats.** Each threat is assessed for probability and severity of occurrence. *Probability* is the estimate of the likelihood that a threat will cause an impact on the mission. Some threats produce losses frequently; others almost never do. *Severity* is the expected consequence of an event in terms of degree of injury, property damage, or other mission-impairing factors (such as loss of combat power). The result of this risk assessment allows prioritization of threats based on risk. The number one risk is the one with the greatest potential impact on the mission. However, the least risky issue may still deserve some attention and, possibly, risk control action. Keep in mind that this priority listing is intended for use as a guide to the relative priority of the risks involved, not as an absolute order to be followed. There may be, as an example, something that is not a significant risk that is extremely simple to control. Figure II-2 depicts the necessary actions.

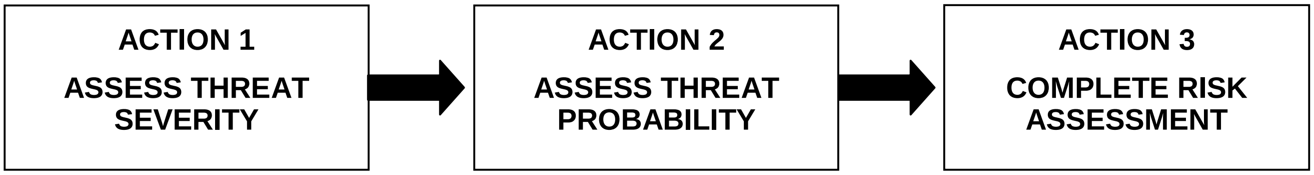


Figure II-2. Assess the Threat

(1) **Action 1—Assess Threat Severity.** Determine the severity of the threat in terms of its potential impact on the mission, exposed personnel, and exposed equipment. Severity categories are defined to provide a qualitative measure of the worst credible outcome resulting from external influence (such as combat or terrorist action; personnel error; environmental conditions; design inadequacies; procedural deficiencies; or system, subsystem, or component failure or malfunction). Severity categories listed in Appendix A, Annex D, provide guidance for a wide variety of missions and systems.

(2) **Action 2—Assess Threat Probability.** Determine the probability that the threat will cause a negative event of the severity assessed in Action 1. Probability may be determined through experienced-based estimates or derived from research, analysis, and evaluation of historical data from similar missions and systems. The typical event sequence is much more complicated than a single line of erect dominos; tipping the first domino (threat) triggers a clearly predictable reaction. Supporting rationale for assigning a probability should be documented for future reference. Generally accepted definitions for probability may be found at Appendix A, Annex D.

(3) **Action 3—Complete Risk Assessment.** Combine severity and probability estimates to form a risk assessment for each threat. When combining the probability of occurrence with severity, a matrix may be used to assist in identifying the level of risk. A sample matrix is in Appendix A, Annex D. Existing databases and/or a panel of personnel experienced with the mission and threats can also be used to help complete the risk assessment.

(4) **Output of Risk Assessment.** The outcome of the risk assessment process is a prioritized list of threats. The highest priority threat is the most serious one to the mission; the last is the least serious risk of any consequence.

(5) **Risk Assessment Pitfalls.** The following are some pitfalls that should be avoided during the assessment:

(a) Over optimism: “It can’t happen to us. We’re already doing it.” This pitfall results from not being totally honest and not looking for root causes of the threats.

(b) Misrepresentation: Individual perspectives may distort data. This can be deliberate or unconscious.

(c) Alarmism: “The sky is falling” approach, or “worst case” estimates are used regardless of their possibility.

(d) Indiscrimination: All data is given equal weight.

(e) Prejudice: Subjectivity and/or hidden agendas are used instead of facts.

(f) Inaccuracy: Bad or misunderstood data nullify accurate risk assessment.

(g) Enumeration: It is difficult to assign a numerical value to human behavior.

- Numbers may oversimplify real life situations.
- It may be difficult to get enough applicable data; this could force inaccurate estimates.
- Numbers often take the place of reasoned judgment.
- Risk can be unrealistically traded off against benefit by relying solely on numbers.

c. **Develop Controls and Make Risk Decisions.** These actions are listed as separate and distinct parts of the overall process by the U.S. Air Force (USAF), but will be dealt with under this overall heading for the purpose of this publication. Figure II-3 depicts the necessary actions.

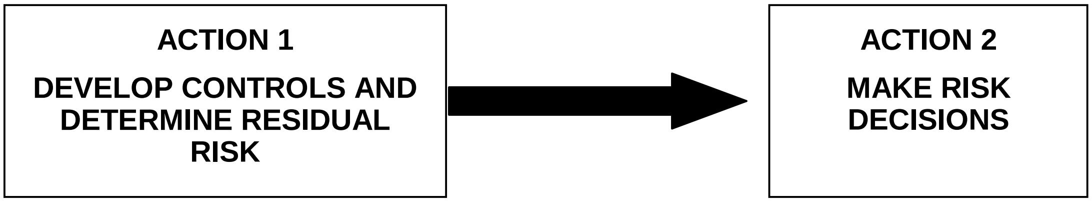


Figure II-3. Develop Controls and Make Risk Decisions

(1) **Action 1—Develop Controls.** After assessing each threat, leaders should develop one or more controls that either eliminate the threat or reduce the risk (probability and/or severity) of threats. For each threat identified, develop one or more control options that either avoid the threat or reduce its risk to a level that meets the commander's risk guidance. Examples of criteria for establishing effective controls are listed in Table II-1.

Table II-1
Criteria for Effective Controls

CONTROL CRITERIA	***REMARKS***
Suitability	Control removes the threat or mitigates (reduces) the residual risk to an acceptable level.
Feasibility	Unit has the capability to implement the control.
Acceptability	Benefit gained by implementing the control justifies the cost in resources and time.
Explicitness	Clearly specifies who, what, where, when, why, and how each control is to be used.
Support	Adequate personnel, equipment, supplies, and facilities necessary to implement a suitable control is available.
Standards	Guidance and procedures for implementing a control are clear, practical, and specific.
Training	Knowledge and skills are adequate to implement a control.
Leadership	Leaders are ready, willing, and able to enforce standards required to implement a control.
Individual	Individual personnel are sufficiently self-disciplined to implement a control.

(a) Some types of controls are as follows:

- **Engineering controls**. These controls use engineering methods to reduce risks, such as developing new technologies or design features, selecting better materials, identifying suitable substitute materials or equipment, or adapting new technologies to existing systems. Examples of engineering controls that have been employed in the past include development of aircraft stealth technology, integrating global positioning system data into cruise missiles, and development of night vision devices.

- **Administrative controls.** These controls involve administrative actions, such as establishing written policies, programs, instructions, and SOPs, or limiting the exposure to a threat either by reducing the number of personnel/assets or length of time they are exposed.

- **Educational controls.** These controls are based on the knowledge and skills of the units and individuals. Effective control is implemented through individual and collective training that ensures performance to standard.

- **Physical controls.** These controls may take the form of barriers and guards or signs to warn individuals and units that a threat exists. Use of personal protective equipment, fences around high power high frequency antennas, and special controller or oversight personnel responsible for locating specific threats fall into this category.

- **Operational controls.** These controls involve operational actions such as pace of operations, battlefield controls (areas of operations and boundaries, direct fire control measures, fire support coordinating measures), rules of engagement, airspace control measures, map exercises, and rehearsals.

(b) A control should avoid/reduce the risk of a threat by accomplishing one or more of the following:

- **Avoiding the risk.** This often requires canceling or delaying the task, mission, or operation and is, therefore, an option rarely exercised because of mission importance. However, it may be possible to avoid specific risks: risks associated with a night operation may be avoided by planning the operation for daytime; thunderstorm or surface-to-air-missile risks can be avoided by changing the flight route.

- **Delay a COA**. If there is no time deadline or other operational benefit to speedy accomplishment of a task, it may be possible to reduce the risk by delaying the task. Over time, the situation may change and the risk may be eliminated, or additional risk control options may become available (resources become available, new technology becomes available, etc.) reducing the overall risk. For example, a mission can be postponed until more favorable weather reduces the risk to the force.

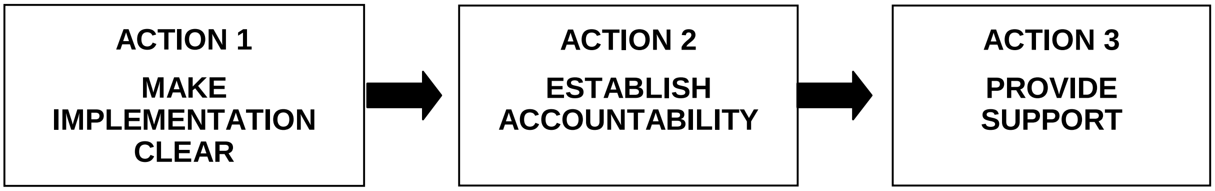
- **Transferring the risk.** Risk may be reduced by transferring a mission, or some portion of that mission, to another unit or platform that is better positioned, more survivable, or more expendable. Transference decreases the probability or severity of the risk to the total force. For example, the decision to fly an unmanned aerial vehicle into a high-risk environment instead of risking a manned aircraft is risk transference.

- **Assigning redundant capabilities.** To ensure the success of critical missions to compensate for potential losses assign redundant capabilities. For example, tasking a unit to deploy two aircraft to attack a single high value target increases the probability of mission success.

(c) **Determine Residual Risk.** Once the leader develops and accepts controls, he or she determines the residual risk associated with each threat and the overall residual risk for the mission. Residual risk is the risk remaining after controls have been identified, selected, and implemented for the threat. As controls for threats are identified and selected, the threats are reassessed, and the level of risk is revised. This process is repeated until the level of residual risk is acceptable to the commander or leader or cannot be further reduced. Overall residual risk of a mission must be determined when more than one threat is identified. The residual risk for each of these threats may have a different level, depending on the assessed probability and severity of the hazardous incident. Overall residual mission risk should be determined based on the threat having the greatest residual risk. Determining overall mission risk by averaging the risks of all threats is not valid. If one threat has high residual risk, the overall residual risk of the mission is high, no matter how many moderate or low risk threats are present.

(2) **Action 2—Make Risk Decisions.** A key element of the risk decision is determining if the risk is justified. The leader should compare and balance the risk against the mission's potential gain. The leader alone decides if controls are sufficient and acceptable and whether to accept the resulting residual risk. If the leader determines the risk level is too high, he or she directs the development of additional or alternate controls, or modifies, changes, or rejects the COA. Leaders can use the risk assessment matrix or other tools found in Appendix A, in conjunction with their commanders' guidance, to communicate how much risk they are willing to allow subordinate leaders to accept.

d. **Implement Controls.** Once the risk control decision is made, assets must be made available to implement the specific controls. Part of implementing controls is informing the personnel in the system of the risk management process results and subsequent decisions. Figure II-4 depicts the actions necessary to complete this step. Careful documentation of each step in the risk management process facilitates risk communication and the rational processes behind risk management decisions.



ACTION 1
MAKE IMPLEMENTATION CLEAR

ACTION 2
ESTABLISH ACCOUNTABILITY

ACTION 3
PROVIDE SUPPORT

Figure II-4. Implement Controls

(1) **Action 1—Make Implementation Clear.** To make the implementation directive clear, consider using examples, providing pictures or charts, including job aids, etc. Provide a roadmap for implementation, a vision of the end state, and description of successful implementation. The control should be presented so it will be received positively by the intended audience. This can best be achieved by designing in user ownership.

(2) **Action 2—Establish Accountability**. Accountability is important to effective risk management. The accountable person is the one who makes the decision (approves the control measures); therefore, the right person (appropriate level) must make the decision. Clear assignment of responsibility for implementation of the risk control is required.

(3) **Action 3—Provide Support.** To be successful, the command must support the risk controls. This support requires—

(a) Providing the personnel and resources necessary to implement the control measures.

(b) Designing in sustainability from the beginning.

(c) Employing the control with a feedback mechanism that will provide information on whether the control is achieving the intended purpose.

e. **Supervise and Review.** Supervise and review involves determining the effectiveness of risk controls throughout the operation. There are three aspects: monitoring the effectiveness of risk controls; determining the need for further assessment of either all, or a portion of, the operation due to an unanticipated change; and capturing lessons learned, both positive and negative. Figure II-5 depicts the necessary actions.

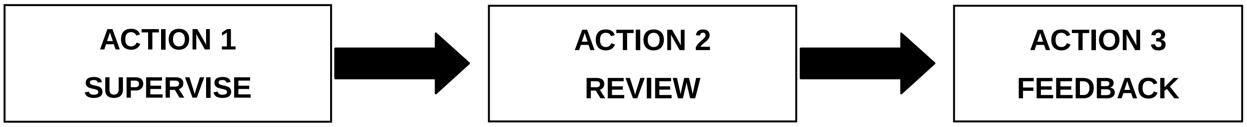


Figure II-5. Supervise and Review

(1) **Action 1—Supervise.** Monitor the operation to ensure—

(a) Controls are implemented correctly, effective, and remain in place.

(b) Changes requiring further risk management are identified.

(c) Action is taken to correct ineffective risk controls and reinitiate the risk management process in response to new threats.

(d) Risks and controls are reevaluated any time the personnel, equipment, or mission tasks change, or new operations are anticipated in an environment not covered in the initial risk management analysis.

Successful mission performance is achieved by shifting the cost versus benefit balance more in favor of benefit through controlling risks. By using risk management whenever anything changes, we consistently control risks identified before an operation and those that develop during the operation. Addressing the risks before they get in the way of mission accomplishment saves resources and enhances mission performance.

(2) **Action 2—Review.** The risk management process review must be systematic. After controls are applied, a review must be accomplished to see if the risks and the mission are in balance. To determine if appropriate risk management controls have been applied, compare METT-T or the 5-M model from the earlier steps to the present risk management assessment.

(a) To accomplish an effective review, commanders identify whether the actual cost is in line with expectations. The commander needs to determine what effect the risk control had on mission performance. It is difficult to evaluate the risk control by itself; therefore, the focus should be on the aspect of mission performance the control measure was designed to improve.

(b) Measurements are necessary to ensure accurate evaluations of how effectively controls eliminated threats or reduced risks. After Action Reports (AAR), surveys, and in-progress reviews provide great starting places for measurements.

(3) **Action 3—Feedback**. A review by itself is not enough; a mission feedback system should be established to ensure that the corrective or preventative action taken was effective and that any newly discovered threats identified during the mission were analyzed and corrective action taken.

(a) When a decision is made to accept risk, factors (cost versus benefit information) involved in the decision should be recorded; proper documentation allows for review of the risk decision process. Then, when a negative consequence occurs, the decision process can be reviewed to determine where errors in the process may have occurred.

(b) Risk analysis will not always be perfect the first time. When errors occur in an analysis, use feedback (such as briefings, lessons learned, cross-tell reports, benchmarking, or database reports) to identify and correct those errors. This feedback will help determine if the previous forecasts were accurate, contained errors, or were completely incorrect.

3. Integration of Risk Management

Tables II-2 and II-3 integrate the risk management process into each phase of the deliberate and crisis action Joint Operation Planning and Execution System (JOPES). The annotations of the joint task force (JTF) and major subordinate element (MSE) in the matrix identify the level of command primarily responsible for risk management execution during each particular phase of planning. The risk management process should be considered throughout the planning process by each level of command.

Table II-2
Risk Management Execution
(Risk Management in Deliberate Planning)

Deliberate Planning	*Identify Threats*	*Assess Threats*	*Develop Controls Make Risk Decision*	*Implement Controls*	*Supervise and Review*
PHASE I Initiation	**JTF**				
PHASE II Concept Development	**JTF**	**JTF**			
PHASE III Plan Development	**MSE**	**MSE**	**JTF** **MSE**		
PHASE IV Plan Review			**JTF**		
PHASE V Supporting Plans	**MSE**	**MSE**	**MSE**	**JTF** **MSE**	
EXECUTION	**JTF** **MSE**	**JTF** **MSE**	**JTF** **MSE**	**JTF** **MSE**	**JTF** **MSE**

Table II-3
Risk Management Execution
(Risk Management in Crisis Action Planning)

CRISIS ACTION PLANNING	***Identify Threats***	***Assess Threats***	***Develop Controls Make Risk Decision***	***Implement Controls***	***Supervise and Review***
PHASE I **Situation Development**	**JTF**	**JTF**			
PHASE II **Crisis Assessment**	**JTF**	**JTF**	**JTF**		
PHASE III **COA Development**	**JTF** **MSE**	**JTF** **MSE**	**JTF** **MSE**		
PHASE IV **COA Selection**			**JTF** **MSE**	**JTF**	
PHASE V **Execution Planning**			**JTF** **MSE**	**JTF** **MSE**	
PHASE VI **Execution**	**MSE**	**MSE**	**MSE**	**JTF** **MSE**	**JTF** **MSE**

4. Analysis Models

a. **The METT-T Model.** The METT-T model can be used for conducting a situation analysis by breaking it into five general areas: (1) the mission itself, (2) the enemy, (3) terrain/weather, (4) troops and support available, and (5) time available.

Note. The U.S. Army uses mission, enemy, terrain and weather, troops and support available, time available, civil considerations (METT-TC), adding civil considerations as a sixth area of analysis.

(1) **Mission.** Leaders first analyze the assigned mission. They look at the type of mission to be accomplished and consider possible subsequent missions. Certain kinds of operations are inherently more dangerous than others. For example, a deliberate frontal attack is more likely to expose a unit to losses than would a defense from prepared positions. Identifying missions that routinely present greater risk is imperative. Leaders also look for threats associated with complexity of the plan (such as a scheme of maneuver that is difficult to understand or too complex for accurate communications down to the lowest level) or the impact of operating under a fragmentary order.

(2) **Enemy.** Commanders look for enemy capabilities that pose significant threats to the operation. For example, “What can the enemy do to defeat my operation?”

(a) Common shortfalls that can create threats during operations include failure to—

- Assess potential advantages to the enemy provided by the battlefield environment.
- Fully assess the enemy’s capabilities.
- Understand enemy capabilities and friendly vulnerabilities to those capabilities.

- Accurately determine the enemy's probable COAs.
- Plan and coordinate active ground and aerial reconnaissance activities.
- Disseminate intelligence about the enemy to lower echelons.
- Identify terrorist threats and capabilities.

(b) Intelligence plays a critical part in identifying threats associated with the presence of an enemy or an adversary. Intelligence preparation of the battlespace is a dynamic staff process that continually integrates new information and intelligence that ultimately becomes input to the commander's risk assessment process. Intelligence assists in identifying threats during operations by—

- Identifying opportunities and constraints the battlefield environment offers to enemy and friendly forces.
- Thoroughly portraying enemy capabilities and vulnerabilities.
- Collecting information on populations, governments, and infrastructures.

(3) **Terrain and Weather.** Terrain and weather pose great potential threats to military operations. The unit must be familiar with both the terrain and its associated environment for a mission to succeed. Basic issues include availability of reliable weather forecasts, how long the unit has operated in the environment and climate, and whether the terrain has been crossed before.

(a) Terrain. The main military aspects of terrain are observation and fields of fire, cover and concealment, obstacles, key terrain, and avenues of approach; these may be used to identify and assess threats impacting friendly forces. Terrain analysis includes both map and visual reconnaissance to identify how well the terrain can accommodate unit capabilities and mission demands.

- *Observation and fields of fire.* Threats associated with observation and fields of fire usually involve when the enemy will be able to engage a friendly unit and when the friendly unit's weapon capabilities allow it to engage the enemy effectively.
- *Cover and concealment.* Threats associated with cover and concealment are created either by failure to use cover and concealment or by the enemy's use of cover and concealment to protect his assets from observation and fire.
- *Obstacles.* Threats associated with obstacles may be caused by natural conditions (such as rivers or swamps) or man-made conditions (such as minefields or built-up areas).
- *Key terrain.* Threats associated with key terrain result when the enemy controls that terrain or denies its use to the friendly forces.
- *Avenues of approach.* Threats associated with avenues of approach include conditions in which an avenue of approach impedes deployment of friendly combat power or conditions that support deployment of enemy combat power.

(b) Weather. To identify weather threats, leaders and unit personnel must assess the impact on operating systems. Threats may arise from—

- Lack of understanding of reliability and accuracy of weather forecasting.
- Effects of climate and weather on personnel and equipment operation and maintenance.
- Effects of weather on mobility.

(4) **Troops and Support Available.** Leaders analyze the capabilities of available friendly troops. Associated threats impact both individual personnel and the unit. Key considerations are level of training, manning levels, the condition and maintenance of equipment, morale, availability of supplies and services, and the physical and emotional health of personnel. All personnel must be vigilant to the fact that threats in these areas can adversely affect a mission. Even when all tactical considerations point to success, mission failure can be caused by—

(a) Threats to physical and emotional health. The health threat depends on a complex set of environmental and operational factors that combine to produce "disease non-battle injuries" as well as combat injuries. Care of troops requires long-range projection of logistical and medical needs with close monitoring of mission changes that could impact troop support.

(b) Threats to task organization or units participating in an operation. Threats include poor communication, unfamiliarity with higher headquarters SOPs, and insufficient combat power to accomplish the mission. How long units have worked together under a particular command relationship should be considered when identifying threats.

(c) Threats associated with long-term missions. Long-term missions include peacekeeping, or insurgency/counterinsurgency operations. Threats associated with these missions include the turmoil of personnel turnover, lack of continuity of leadership, inexperience, and lack of knowledge of the situation and the unit's operating procedures. Long-term missions can also lead to complacency; units conditioned to routine ways of accomplishing the mission fail to see warnings evident in the operational environment. An especially insidious threat is the atrophy of critical-skills that results from not performing mission-essential task list related missions.

(5) **Time Available.** The threat is insufficient time to plan, prepare, and execute operations. Planning time is always at a premium. Leaders routinely apply the one-third/two-thirds rule (providing two thirds of time available to subordinates for planning) to ensure their subordinate units are given maximum time to plan. Failure to accomplish a mission on time can result in shortages of time for subordinate and adjacent units to accomplish their missions.

b. **U.S. Army Situation Analysis.** While Joint, Marine Corps, Air Force, and Navy doctrine use METT-T for situation analysis, the Army uses METT-TC. The "C" in METT-TC is civil considerations—how the attitudes and activities of the civilian leaders, populations, and organizations within an area of operations will influence the conduct of military operations. Threats associated with civil considerations include, but are not limited to, collateral damage, changing political and social attitudes, civilian unrest, the influence of the press on public opinion, conflicting goals and objectives of private voluntary organizations (PVOs) and nongovernmental organizations (NGOs), and the handling of refugees, noncombatants, and protesters.

c. **5-M Model.** The 5-M model provides an alternative framework for conducting mission analysis by examining the impacts and inter-relationships between the composite elements of Man, Machine, Media, Management, and Mission. The amount of overlap or interaction between the individual components is a characteristic of each mission and evolves as the mission develops.

(1) **Man.** This is the area of greatest variability and thus possesses the majority of risks. Some considerations and potential threats are listed in Table II-4.

Table II-4
Considerations and Potential Threats Analyzed
(Man Element, 5-M Model)

Considerations	***Potential Threats***
Selection	Wrong person psychologically/physically, not proficient in assigned task, no procedural guidance
Performance	Lack of awareness, false perceptions, over-tasking, distraction, channelized attention, stress, peer pressure, over/lack of confidence, poor insight, poor adaptive skills, pressure/workload, fatigue
Personal Factors	Expectations, lack of job satisfaction, poor values, families/friends, command/control, poor discipline (internal and external), perceived pressure (over tasking) and poor communication skills

(2) **Machine.** Used as intended, limitations interface with man. Some considerations and potential threats are listed in Table II-5.

Table II-5
Considerations and Potential Threats Analyzed
(Machine Element, 5-M Model)

Considerations	***Potential Threats***
Design	Engineering reliability and performance, ergonomics
Maintenance	Availability of time, tools, and parts, ease of access
Logistics	Supply, upkeep, and repair
Technical Data	Clear, accurate, useable, and available

(3) **Media.** This includes external, largely environmental forces. Some considerations and potential threats are listed in Table II-6.

Table II-6
Considerations and Potential Threats Analyzed
(Media Element, 5-M Model)

Considerations	***Potential Threats***
Climatic	**Ceiling, visibility, temperature, humidity, wind, and precipitation**
Operational	**Terrain, wildlife, vegetation, man-made obstructions, daylight, maritime environment, and darkness**
Hygienic	**Ventilation/air quality, noise/vibration, dust, and contaminants**
Trafficability	**Pavement, gravel, dirt, ice, mud, dust, snow, sand, hills, and curves**

(4) **Management.** Directs the process by defining standards, procedures, and controls. While management provides procedures and rules to govern interactions, it cannot completely control the system elements. For example, weather is not under management control and individual decisions affect off-duty personnel much more than management policies. Some considerations and examples are listed in Table II-7.

Table II-7
Management Tools and Examples Analyzed
(Management Element, 5-M Model)

Considerations	***Examples***
Standards	**Doctrine statements, applicable criteria, and policy directives**
Procedures	**Checklists, SOPs, work cards, and multi-command manuals**
Controls	**Crew rest, altitude/airspeed/speed limits, restrictions, training rules/limitations, rules of engagement (ROE), lawful orders**

(5) **Mission.** The desired outcome. Objectives: Big picture understood, well defined, obtainable. The results of the interactions of the other 4-Ms (Man, Media, Machine, and Management).